REMARKS

Applicant has amended the specification to reference designations and replace them with "(not shown)" since the attacking computer and the ISP are not shown nor are they needed to be shown in FIG. 1.

At the outset Applicant seeks clarification. In response to applicant's arguments, the examiner stated:

> **2. Applicant's arguments with respect to the Katz reference in the rejections of claims 1-1 3, 15, 17-1 9 and 21 (p. 7, 2nd par.) have been considered but are not persuasive. Applicant's amendments have necessitated a new search and new grounds of rejection.**

Applicant contends that Applicant's arguments with respect to Katz in the rejections of claims 1-13, 15, 17-19 and 21 were persuasive, since the examiner conducted a new search and new grounds of rejection and removed Katz as a reference against these claims.

The examiner objected to claim 2. Applicant has amended claim 2 to overcome the objection.

The examiner rejected claim 11 under 35 U.S.C. 112, second paragraph as being indefinite. Applicant has corrected claim 11.

The examiner rejected Claims 1-3, 5-8, 10-13, 15, 17-19 and 21-22 under 35 U.S.C. 103(a), as being unpatentable over Mansfield ("Towards Trapping Wily Intruders in the Large") in view of Mell et al ("Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems").

The examiner rejected Claims 1-3, 5-8, 10-13, 15, 17-19 and 21-22 under 35 U.S.C. 103(a), as being unpatentable over Mansfield ("Towards Trapping Wily Intruders in the Large") in view of Mell et al ("Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems").

Claim 1 is allowable since the references neither describe nor suggest *** a computing device that samples packet traffic over a network, and which accumulates and collects statistical information about the packet traffic *** and a port to link the data collector over a redundant

network that does not carry the packet traffic to deliver the accumulated and collected statistical *** .

Claims 2-3, 5-8, 10-13, 15, 17-19 and 21-22 are distinct over Mansfield in view of Mell et al., since the references neither separately nor in combination suggest the combination of instructions to perform sampling and statistic collection of data pertaining to network packets; parse the information in the sampled packets and maintain the information in a log, and a port to link the data collectors over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center.

The examiner admits that: "Mansfield does not disclose utilizing a redundant network that does not carry the packet traffic to deliver the generated statistics to a central control center." (Office Action page 5). The examiner relies on Mell to teach "utilizing a separate and protected network for communications between data collectors and a control center (Section 2.0, Background on Distributed Hierarchical IDSs; Section 3.0, Vulnerable Systems).," The examiner contends that:

> **It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Mansfield method to utilize a separate and protected network for communications between the data collector and the control center, as taught by Mell, so that the data collector would not be isolated in the event an attacker floods the communication channel on which the data collector is residing.**

Mell discloses mobile agent attack resistant distributed hierarchical intrusion detection systems. According to Mell, a solution to the problem related to the vulnerability of distributed intrusion detection systems is to cast the internal nodes in the system hierarchy as mobile agents. These mobile agents randomly move around the network such that an attacker can not locate their position.

Mell in (Section 2.0, Background on Distributed Hierarchical IDSs; Section 3.0, Vulnerable Systems) discloses:

> **2.0 Background on Distributed Hierarchical IDSs**
>
> **Commercial IDSs are migrating towards a distributed hierarchical architecture. The architecture is a tree with a command and control system at the**

top, information aggregation units at the internal nodes, and operational units at the leaf nodes. The operational units can be network sniffing IDSs, host based IDSs, virus checkers, and various attack response systems.Attack detection and information gathering occurs at the leaf nodes. That information is passed to an internal node that aggregates information from multiple leaf nodes. Further aggregation, abstraction, and data reduction occurs at higher internal nodes until the root is reached. The root is a command and control system that evaluates attack situations and often issues responses. The root usually reports to human user consoles that can manually issue responses and evaluate the network..This architecture is excellent for creating scalable distributed IDSs with central points of administration. However, the static placement of the non-leaf nodes in this architecture makes them vulnerable to attackers.

3.0 Vulnerable Systems

Most commercial IDSs and many research IDSs have this vulnerable architecture. Examples of products with distributed hierarchical architectures are: UC Davis's GrIDS [CHEN96], Lawrence Livamore's SPI-NET [SPIN99], Cisco's NetRanger WIX], Axent's Intruder Alert m]In,te rnet Security System's Realsecure [REAL], Network Associates Incorporated's Active Security [ACTI], and Purdue's AAFID [BALA98]. It is not our intention to state that these products are vulnerable to attack. Indeed, most developers implement very tight security in their IDS nodes in order to prevent outside penetration. However, it is currently infeasible to formally prove the security of such systems and so vulnerabilities still may exist. More importantly, many denial of service attacks are effective against perfectly implemented systems. If an attacker can send the target more information than the target can handle then it will cease to function. In addition, if an attacker floods communication channel on which an IDS node is residing, the IDS node is cut off from the rest of the virtual IDS network. These vulnerability exists regardless of the protections implemented on the IDS node. One solution to this problem is to provide IDSs a separate and protected communication channel for their operation. This solution works well but is very costly, as separate cables must be run for the IDS system. Our solution using mobile agents provides a solution to this problem without having to have separate protected communication channels for IDS nodes. However, our solution has its own set of requirements and assumptions.

It would not be suggestion to one of ordinary skill in the art, to modify Mansfield with Mell to provide the claimed feature of a port to link the data collector over a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center.

Mell clearly teaches away from providing "IDSs a separate and protected communication channel for their operation." contrary to the position taken by the examiner since, Mell clearly states: "This solution works well but is very costly, as separate cables must be run for the IDS system. Our solution using mobile agents provides a solution to this problem without having to have separate protected communication channels for IDS nodes." Mell clearly teaches away from the teachings in 3.0. In addition, Mell does not teach the control center.

Mansfield teaches in section 5:

> **The traffic monitoring is carried out using agents which watch all the traffic but process only the suspicious packets. The agents can be accessed, queried and configured using the standard SNMP management protocol. The Security Manager system is alerted on the detection of potential attempts. The Security Manager uses the network configuration information to trap and/or track-down the intruder. The communication between the different Manager's and the agents is carried out using the standard SNMP management protocol.**

This teaching does not suggest the control center feature of Applicant's claim 2. At the outset, Mansfield does not suggest that the data collectors deliver the accumulated and collected statistical information about the network packet traffic to the control center. Rather, Mansfield teaches to that the "Security Manager system is alerted on the detection of potential attempts." To the extent that the examiner considers the Security Manager as the central control center, the Security Manager does not receive the data recited in claim 1, but rather is alerted on the detection of potential attempts, suggesting to one of skill that the agents process data looking for attempts. Mansfield confirms this where Mansfield states: "The traffic monitoring is carried out using agents which watch all the traffic but process only the suspicious packets." (Mansfield Section 5.). Moreover, Mansfield also discloses that communications occur between "different Managers and the agents" using the standard SNMP management protocol. Thus, Mansfield does not suggest a central controller, as recited in claim 2.

Mell on the other hand does not suggest a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center.

Mell discusses conventional IDS's and shows a hierarchical distributed arrangement in FIG. 1.

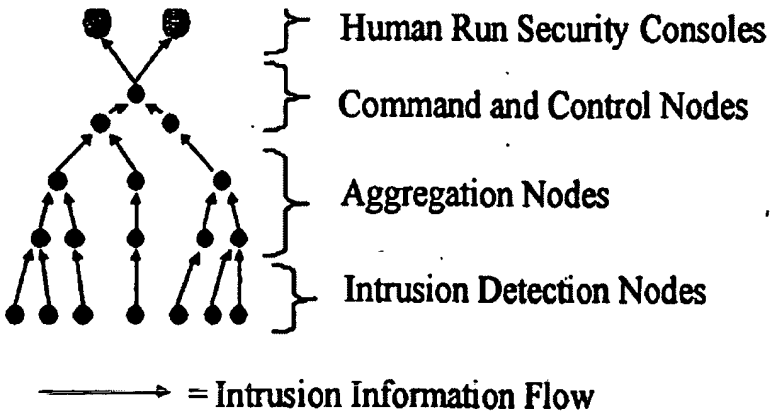

Figure 1: Generic Distributed Hierarchical Intrusion Detection Architecture

Mell, like Mansfield, does not disclose the control center feature of Applicant's claim 1 nor does Mell suggest a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center.

Applicant also contends that there is no suggestion to combine the teachings of Mell with Mansfield. The examiner's proffered motivation is to "utilize a separate and protected network for communications between the data collector and the control center, as taught by Mell, so that the data collector would not be isolated in the event an attacker floods the communication channel on which the data collector is residing." However, that motivation is of no consequence to Mansfield, since Mansfield is a study of features of different types of attacks. The examiner has failed to show how Mansfield, which is directed to features of types of attacks, would be benefited by the teachings of Mell, where Mansfield does not describe any architecture or device to deal with the attacks.

Accordingly, the motivation to modify Mansfield to include a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center is not present. Therefore, claim 2 is allowable over the references.

Claims 3, 5-8, and 10 depend directly or indirectly on claim 2 and are allowable with claim 2.

Claims 11-13, 15, 17-19 and 21-22 are also allowable because they each include a similar limitation of a port to link the data collectors over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center.

The examiner rejected Claim 14 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell, as applied to claim 13, and further in view of Zait et al., U.S. Patent 6,665,684.

Claim 14 further limits the method of claim 13 by dividing the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter and adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets.

The examiner contends that Mansfield teaches "dividing the traffic flow and using memory spaces to track counts of how many packets a data collector examines for a given parameter (p5, 1st par). ..." In this passage cited by the examiner, Mansfield is merely discussing setting thresholds to see how many related packets are received in order to catch low rate scanner attacks. Mansfield neither describes nor suggests to divide the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter. The examiner admits that Mansfield does not disclose: "adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets" and instead relied on Zait for this teaching.

However, Zait neither describes nor suggests dividing the traffic flow into buckets nor adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets. Zait is directed to database table partitioning. Zait discusses three types of partitions "hash-based partitioning and range-based partitioning" (Col. 4 lines 11-12) and a composite partition. (Col. 4 line 10) Zait describes that: "with range-based partitioning, it becomes necessary to add new partitions when newly arriving rows have partition key values that fall outside the ranges of existing partitions." (Col. 4 lines 13-16) Zait describes that: "... all partition key values fall within existing partitions of a hash-partitioned table. However, it may be desirable to add new partitions to a hash-partitioned table, for example, to spread the data over a greater number of devices." (Col. 4 lines 22-26) Zait describes a composite technique of range and hash based partitions.

However, the partitions that Zait discusses are records in a table, e.g., to divide a table of records according to some criteria to make data base management, e.g., improving access to objects (Col. 3 lines 44-45).

Neither Zait nor Mansfield nor Mell suggest the desirability of dividing the traffic flow into buckets that track counts of packets examined for a given parameter and adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets. Neither appreciates the problem of an attack that exploits memory space. Zait teaches database management, and is not concerned with attacks that exploit memory space. Mansfield although addressing techniques to address attacks does not recognize the problem of attacks that exploit memory space. Accordingly, claim 14 is allowable over the art, since the combination of references do not suggest the claimed elements and further that there is no suggestion to combine the references.

The examiner rejected Claim 16 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 15, and further in view of Roesch "Snort-Lightweight Intrusion Detection for Networks."

At the outset applicant notes that the examiner mentions Katz in the body of the rejection, but does not mention Katz in the summary of the rejection or in the earlier rejections. Applicant will not deal with Katz since no specific argument is directed to Katz.

Claim 16 limits claim 15 by requiring that the layer 3-7 analysis involves monitoring network traffic for unusual levels of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets.

Claim 16 is allowable at least for the reasons discussed in base claim 15. In addition, Roesch describes reassembly of fragments to allow full payload decoding and alerting in the presence of packet fragments smaller than a predetermined size. Claim 16 recites monitoring for unusual levels of IP fragmentation (that is, more fragmented packets, of any size, than would normally be expect on the network), and detection of fragments with invalid or overlapping fragment offsets. As such, Roesch neither describes nor suggests the features of claim 16.

The examiner rejected Claim 20 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 15, and further in view of Eichstaedt et al., U.S. Patent 6,662,230.

Again, the examiner has not addressed any argument that relies on Katz.

Claim 20 further limits claim 15 by reciting that the layer 3-7 analysis includes monitoring network traffic for an indication of a frequency of re-load requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. The examiner admits that neither Mansfield nor Katz address this feature, and instead turns to a reference Eichstaedt that pertains to web robots or web-crawlers that obtain documents from a web server.

Initially, applicant notes that claim 20 is directed to a method of collecting data from sampled network traffic, not collecting web pages from a server as taught by Eichstaedt. Eichstaedt teaches to allow a server to limit access to client systems (Col. 6, lines 21-39). Eichstaedt is not concerned with monitoring network traffic for an indication of a frequency of reload requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. Eichstaedt also does not provide any motivation or solution suitable in the context of Mansfield and Katz or claim 20. While Eichstaedt teaches to limit access to client systems (Col. 6, lines 21-39), such a solution is of no import to an intrusion detection system, as taught by the references. Accordingly, whether taken separately or in combination there is no suggestion in Eichstaedt nor the other cited art of monitoring network traffic for an indication of a frequency of reload requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. Therefore, claim 20 is also allowable.

The examiner rejected Claims 1-13 and 21 under 35 U.S.C. 103(a) as being unpatentable over Stallings "Cryptography and Network Security: Principles and Practice," in view of Mell et al.

Claims 1-13 and 21 are distinct over Stallings in view of Mell et al., since the references neither separately nor in combination suggest the combination of instructions to perform

sampling and statistic collection of data pertaining to network packets; parse the information in the sampled packets and maintain the information in a log, and a port to link the data collectors over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center.

The examiner contends that Stallings teaches "sampling the network traffic and generating statistics about the network flow," and acknowledges that "Stallings does not disclose utilizing a hardened, redundant network. The examiner relies on Mell to teach this feature, using the same motivation in the rejection based on Mansfield and Mell.

Applicant contends that Stallings and Mell neither describe nor suggest whether taken together or separately, claim 2.

Stallings is directed to intrusion detection systems. Stallings has no relevant teachings related to statistical data. In Stallings, so called audit collection process produces audit records that are filtered to retain records of interest. Stallings does not suggest of instructions to perform sampling and statistic collection of data pertaining to network packets nor a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic *** .

Applicant also contends that a combination of the teachings of Mell with Stallings, simply provides an intrusion detection system and fails to provide all of the features of claim 2. Accordingly, claim 2 is allowable over the references.

The examiner rejected Claim 4 under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Mell and official notice.

Claim 4 is allowable at least for the reasons discussed in claim 1.

Applicant has enclosed an Information Disclosure Statement. Applicant contends that the claims are allowable over the art in the IDS and the art of record. Accordingly, allowance of the application is requested.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 7/26/05

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21094238.doc